10593/02/DE
WP 73

Arbeitsdokument zur elektronischen Verwaltung (*E-Government*)

Angenommen am 8. Mai 2003

DIE GRUPPE FÜR DEN SCHUTZ VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN,

eingesetzt nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995[1],

gestützt auf Artikel 29 sowie Artikel 30 Absatz 1 Buchstabe a) und Absatz 3 jener Richtlinie,

gemäß den Verfahrensregeln jener Richtlinie und insbesondere der Artikel 12 und 14

HAT FOLGENDES ARBEITSDOKUMENT ANGENOMMEN:

EINLEITUNG

Die Entwicklung der elektronischen Verwaltung stellt heute in den meisten Mitgliedstaaten einen der wesentlichen Schwerpunkte bei der Modernisierung ihrer Verwaltungen dar. Auf europäischer Ebene äußert sich diese Priorität in der Verabschiedung des „Aktionsplans e-Europe 2002“ mit einem Kapitel „Online-Verwaltung“ durch den Europäischen Rat von Feira im Juni 2000.

Entsprechend sind zurzeit verschiedene Typen von Projekten zur elektronischen Verwaltung zu beobachten, welche die Einrichtung und die Förderung der Online-Abwicklung von Verwaltungsverfahren zum Gegenstand haben. Offenbar stellen sich bei einigen Projekten komplexe Fragen zum Datenschutz, die sorgfältig geprüft werden müssen, wenn die Projekte zur elektronischen Verwaltung erfolgreich eingeführt werden sollen.

Beispiele sind etwa die Einrichtung eines einheitlichen Einstiegspunkts zu den Angeboten der Online-Verwaltung, individuelle Kennziffern oder die Einführung des Datenaustauschs zwischen öffentlichen Datenbanken.

Dieses Dokument möchte die aktuelle Situation im Bereich der elektronischen Verwaltung (*E-Government*) sowie in Bezug auf den Schutz der personenbezogenen Daten von Einzelpersonen in der Europäischen Union darstellen und soll zur Diskussion über dieses Thema beitragen. Das von der französischen Vertretung erstellte Dokument fasst die Antworten auf einen Fragebogen zusammen, die von den in der Datenschutzgruppe vertretenen Datenschutzbehörden vorgetragen wurden.

In Anbetracht der konstanten Entwicklung von Angeboten der elektronischen Verwaltung und der Schlussfolgerungen aufgrund von Erfahrungen in diesem Bereich könnte die Datenschutzgruppe später auf diese Fragen zurückkommen, um in diesem Zusammenhang weiter gehende Hilfestellung zur Umsetzung der Bestimmungen der Richtlinie 95/46/EG bieten zu können.

---

[1] Amtsblatt Nr. L 281 vom 23.11.1995, S. 31, verfügbar unter http://europa.eu.int/comm/internal_market/en/dataprot/index.htm

A. ANHÖRUNGEN UND INITIATIVEN DER DATENSCHUTZBEHÖRDEN ZU FRAGEN DER ELEKTRONISCHEN VERWALTUNG

Alle europäischen Datenschutzbehörden haben auf die eine oder andere Art ihre Standpunkte zu Fragen der elektronischen Verwaltung zum Ausdruck gebracht.

1. In der großen Mehrheit aller Fälle wurden die Datenschutzbehörden offiziell von den öffentlichen Stellen hinzugezogen. Im Allgemeinen sind die entsprechenden Beratungen im Rahmen der von den nationalen Datenschutzbestimmungen vorgesehenen Verfahren für die Verwaltungen förmlich vorgeschrieben, wenn die Verwaltungen legislative oder regulierende und für den Datenschutz erhebliche Maßnahmen treffen, bzw. wenn bestimmte Verfahren der Online-Verwaltung eingeführt werden. Diesbezüglich haben verschiedene Datenschutzbehörden erklärt, dass die öffentlichen Behörden ihrer Verpflichtung zur Anhörung der Datenschutzbehörden nicht systematisch nachkommen. Die Verwaltungen konnten die Datenschutzbehörden in Angelegenheiten der elektronischen Verwaltung aber auch spontan anhören.

2. Außerdem konnten die Datenschutzbehörden ihre Standpunkte in öffentlichen Debatten sowie in Fällen darstellen, in denen sich öffentliche Stellen im betreffenden Zusammenhang äußerten. In Frankreich z.B. wurde die CNIL von der Regierung in die öffentliche Diskussion dieser Fragen einbezogen; die CNIL veröffentlichte ihre Überlegungen zu diesem Thema im letzten CNIL-Jahresbericht; im Vereinigten Königreich äußerte der *Information Commissioner* (der von den öffentlichen Stellen nicht förmlich angehört wurde) Kommentare zu verschiedenen Vorschlägen der Regierung oder beteiligte sich an öffentlichen Anhörungen.

3. Die Datenschutzbehörden haben sich verschiedentlich auch aus eigener Initiative zu Fragen der elektronischen Verwaltung geäußert. In den Niederlanden hat die Datenschutzbehörde z.B. ohne ausdrücklichen Anlass ihre Standpunkte zu den entsprechenden Fragen zum Ausdruck gebracht.

4. Und schließlich konnten die Datenschutzbehörden Arbeitsgruppen zu bestimmten Projekten im Bereich der elektronischen Verwaltung angehören (Finnland, Niederlande und Frankreich insbesondere) oder haben darum gebeten, über die Entwicklung bestimmter Projekte informiert zu werden (Portugal).

Die Anhörungen und Initiativen der Datenschutzbehörden konnten sich auf den allgemeinen Rahmen der Entwicklung der elektronischen Verwaltung beziehen, aber auch besondere Fragen zum Gegenstand haben.

Die Beiträge der verschiedenen Vertretungen zeigen, dass die Datenschutzbehörden sehr unterschiedliche Fragen behandelt haben. Die Stellungnahmen können sich zunächst einmal auf Gesamtprojekte beziehen: in Spanien z.B. auf die Einführung eines elektronischen Ausweises oder auf die Einführung eines allgemeinen Projektes zur Förderung der elektronischen Verwaltung, in Schweden auf die Einführung einer „allgemeinen Politik“ der Schwedischen Bankenvereinigung und der Post betreffend den elektronischen Ausweis und in Italien außer auf die Einführung eines elektronischen Ausweises auch auf die Einführung eines nationalen Projektes zur Einrichtung eines

„einheitlichen Netzes der öffentlichen Verwaltung“, d.h. eines elektronischen Netzes zur Verbindung aller Verwaltungsbehörden des Landes.

Ebenso haben Datenschutzbehörden aber auch Einschätzungen zur Umsetzung bestimmter Verfahren der Online-Verwaltung dargelegt: Einschätzungen betreffend Personensteuern, die Online-Einkommenssteuererklärung und die Online-Überweisung von Steuerzahlungen, die soziale Sicherheit, die Online-Erklärung und -Rückerstattung von Gesundheitsausgaben (Spanien, Frankreich) usw. Im Zusammenhang mit diesen Themen bestehen die Behörden insbesondere auf dem Aspekt der Datensicherheit.

Ferner wurden Bewertungen zur Umsetzung bestimmter Texte wie z.B. der Europäischen Richtlinie zu elektronischen Signaturen in nationales Recht geäußert (insbesondere in Finnland, wo das Übergangsgesetz am 1. Februar 2003 in Kraft tritt, sowie in Dänemark, wo die Datenschutzbehörde einen Gesetzesentwurf zu dieser Angelegenheit vorgelegt hat, und in Spanien, wo die Datenschutzbehörde einen Bericht über einen Gesetzesentwurf veröffentlicht hat).

B. ENTWICKLUNG DER ÖFFENTLICHEN VERFAHREN DER ONLINE-VERWALTUNG

Mit dieser Frage sollte für die Liste der 20 grundlegenden Verwaltungsverfahren, die gemäß dem Aktionsplan e-Europe des Europäischen Rats von Feira (Juni 2000) online angeboten werden sollten, sowie für die entsprechend umgesetzten Sicherheitsvorkehrungen der Entwicklungsstand in den einzelnen Ländern festgestellt werden. Nur acht Länder füllten die entsprechende Tabelle aus.

Außer in Belgien und in Deutschland wurden alle Datenschutzbehörden zu den Projekten in Verbindung mit Verfahren der Online-Verwaltung angehört, die in den jeweiligen Ländern eingeführt wurden.

Im Allgemeinen stehen die Beobachtungen der Datenschutzbehörden vorwiegend mit Sicherheitsvorkehrungen und insbesondere mit Maßnahmen zur Identifizierung und zur Authentifizierung von Benutzern und von Vertretern oder beruflichen Nutzern in Verbindung, denen Zugriff auf Anwendungen zur Nutzung der Verfahren der Online-Verwaltung gewährt wurde. Ebenso stellen die Verschlüsselung der Daten während der Übertragung sowie - in geringerem Umfang - die Verschlüsselung bei der Datenspeicherung und die Einrichtung von Protokollsystemen und von Protokolldateien (Portugal, Niederlande, Frankreich und Österreich) allgemein empfohlene Sicherheitsvorkehrungen dar.

Darüber hinaus stimmen die Datenschutzbehörden darin überein, dass die Entwicklung von Verfahren der Online-Verwaltung von Maßnahmen zur Aufklärung der Bürger, insbesondere hinsichtlich der ihnen gemäß den Datenschutzvorschriften garantierten Rechte, begleitet sein muss.

1. Zunächst einmal ist festzustellen, dass alle genannten Länder dem Bürger ein Verfahren zur Online-Übermittlung der Einkommenssteuererklärung anbieten, häufig in Verbindung mit einem Verfahren der Online-Zahlung (sechs Länder) und zur Online-Abfrage der jeweils eigenen Daten (fünf Länder).

Ebenso steht auch bei den für Unternehmen verfügbaren Verfahren der Online-Verwaltung die Online-Steuererklärung im Vordergrund (in acht Ländern die Umsatzsteuererklärung und in sechs Ländern die Erklärung direkter Steuern).

Die elektronische Verwaltung kommt somit zweifellos vorzugsweise im Bereich der öffentlichen Finanzen zum Tragen**.** Dabei ist festzuhalten, dass bei den Verfahren der Online-Verwaltung in diesem Bereich im Allgemeinen eine höhere Sicherheitsstufe besteht als bei sonstigen Verfahren der Online-Verwaltung; verschiedene Länder berichten über den Einsatz elektronischer Signaturen (Finnland, Spanien und Frankreich) sowie über Datenverschlüsselungen (Frankreich, Portugal und Spanien). In Österreich beschränkt sich der Zugriffsschutz auf die Überprüfung von Kennwörtern.

2. Nach den Anwendungen im Steuerwesen werden Umzugsmeldungen (in vielen Ländern ein normaler, förmlicher (bzw. sogar verbindlich vorgeschriebener) Verwaltungsvorgang) am häufigsten als Verfahren der Online-Verwaltung genannt. Sechs Länder erklären, dass dieses Angebot bestehe[2], und in drei Ländern (Spanien, Finnland, Norwegen) wird dieses Angebot um die Möglichkeit der Online-Überprüfung der personenbezogenen Daten ergänzt. Bei diesen Diensten werden von Land zu Land unterschiedliche Sicherheitsstufen eingesetzt; in manchen Ländern (Spanien und Finnland) werden elektronische Signaturen verwendet.

3. Ferner wird die Stellenvermittlung als Online-Verfahren genannt (in sechs Ländern)[3]; dieses Angebot wird verschiedentlich mit der Möglichkeit der Online-Abfrage der personenbezogenen Daten verbunden (drei Länder). Diese Verfahren sind im Allgemeinen durch die Abfrage eines Benutzernamens und eines Kennworts (d.h. durch herkömmliche Sicherheitsfunktionen) geschützt.

   Außerdem werden folgende Online-Verfahren genannt: Einreichen von Bauanträgen, Leihverfahren in öffentlichen Bibliotheken, Anträge in bestimmten Abteilungen der Grundbuchämter, Registrierung von Unternehmensgründungen, Sozialsteuern, Kommunikation mit Gesundheitseinrichtungen und mit Vertretern und Beschäftigten des Gesundheitswesens, Anmeldungen in Schulen und Einschreibungen in Universitäten, Anmeldungen zu Prüfungen, Kfz-Anmeldungen, Rückerstattung medizinischer Aufwendungen, Geltendmachung von Ansprüchen und Einreichen von Beschwerden und Klagen bei Polizei, Justiz usw. (in der Regel unter gleichzeitiger Übermittlung auf dem Postwege) usw...

   Bei der Analyse der von den Datenschutzbehörden übermittelten Antworten zur Sicherheit der genannten Verfahren der Online-Verwaltung zeigen sich erhebliche Unterschiede; eine Ausnahme bilden einige Angebote, die zu Recht als „sensibler“ betrachtet werden (z.B. Kfz-Anmeldungen oder die Behandlung medizinischer Aufwendungen), und für die bestimmte Sicherheitsvorkehrungen von Vorteil zu sein scheinen. Mit Ausnahme der Feststellung, dass bislang noch kein Land - außer vielleicht Finnland und Dänemark - eine klare und fundierte Vorstellung von den Sicherheitsanforderungen an Anwendungen der elektronischen Verwaltung besitzt, sind wesentliche Schlussfolgerungen also noch nicht möglich.

---

[2] Dänemark, Spanien, Finnland, Italien, Norwegen, Niederlande

[3] Dänemark, Finnland, Frankreich, Italien, Norwegen, Portugal

C. EINRICHTUNG EINES EINHEITLICHEN EINSTIEGS (ODER „PORTALS“) FÜR VERFAHREN DER ONLINE-VERWALTUNG

1. Allgemeines

Der „Portal“-Ansatz, d.h. die Entwicklung eines einheitlichen Einstiegs für alle Verfahren der Online-Verwaltung, wurde in fast allen in dieser Studie berücksichtigten Ländern bereits umgesetzt bzw. soll umgesetzt werden. Diese allgemeine Tendenz ist in den Ländern zu verzeichnen, in denen sich die Sites mehr oder weniger als unabhängige Portale entwickelt haben, bzw. in Ländern, in denen bislang noch keinerlei System bestand.

In manchen Fällen ist ein bestimmtes Ministerium für das Portal zuständig. In Finnland z.B. untersteht die Site http://www.suomi.fi dem Finanzministerium, und auch in Österreich wird das Portal der Bundesregierung (http://www.help.gov.at) vom Finanzministerium verwaltet.

Diese Portale sind im Allgemeinen Sites mit umfassenden Angeboten: Verknüpfungen zu den verschiedenen Angeboten der öffentlichen Hand und der Institutionen, Verzeichnisse der Anschriften von Verwaltungsstellen und öffentlichen Einrichtungen, Informationsdateien, Auszüge aus den Amtsblättern betreffend bestimmte Prozesse (Formulare, Informationen zu Verwaltungsverfahren und zu Fördermöglichkeiten, Förderanträge, Ausschreibungen, Stellenangebote der öffentlichen Hand usw.), Informationen zu nationalen Rechtsvorschriften, aktuelle Ereignisse, Briefkästen für Rückmeldungen der Benutzer, Veröffentlichungen usw.

Zunehmend häufiger werden diese Portale sowohl von den Bürgern als auch von den Unternehmen als Zugang zu Verfahren der Online-Verwaltung genutzt. Entsprechend stellt sich die Frage der möglichen Speicherung personenbezogener Daten in den Portalen. Zurzeit werden in diesen Sites in Dänemark, Deutschland, Spanien, Portugal und Schweden keine personenbezogenen Daten gespeichert. In Belgien, Italien, Norwegen, Finnland, Österreich und Irland verfügen diese Sites jedoch über die Möglichkeit (bzw. werden über die Möglichkeit verfügen), personenbezogene Daten zu speichern; in Österreich besteht diese Möglichkeit allerdings nur in Verbindung mit Verfahren, bei denen eine Identifizierung der Bürger tatsächlich unumgänglich ist.

In Irland bietet das System die Möglichkeit der Online-Registrierung. Das System beinhaltet eine Authentifizierung der jeweiligen Benutzeridentität mit Hilfe der PPSN (*Public Service Number*) der betreffenden Person sowie die über einen Makler angebotenen Verwaltungsverfahren, wobei der Makler personenbezogene Daten in einem sicheren Datenspeicher erfasst. Die Identität der betreffenden Benutzer wird in der *Public Service Identity*-Datenbank überprüft, die dem Ministerium für Soziales und Familie untersteht. Bei Transaktionen mit höheren Sicherheitsanforderungen und vertraulicheren Inhalten führt das System eine weiter gehende Authentifizierung durch.

Die Benutzer müssen sich *individuell* damit einverstanden erklären, dass sie über einen Makler auf die betreffenden Angebote zugreifen, und die Bürger können bestehende Angebote auch unabhängig von diesem System nutzen. Häufig benötigte personenbezogene Daten (z.B. Geburtsdatum, Kennwörter, Einkommen, Familienbeziehungen usw.) werden vom Makler in einem zentralen Datenspeicher verwaltet. Der Makler verwaltet diese Informationen und schützt die Informationen im Interesse der Benutzer. Die entsprechenden Daten werden öffentlichen Behörden

ausschließlich auf ausdrückliche Anweisung des an einer Transaktion beteiligten Benutzers über den Makler zugänglich gemacht. Für die verschiedenen Angebote werden jeweils geeignete Sicherheitsvorkehrungen entwickelt, und die personenbezogenen Daten im Datenspeicher werden verschlüsselt.

Bei entsprechendem Entwicklungsstand des Systems kann der Makler feststellen, welche Ereignisse im Leben eines Benutzers gerade anstehen (z.B. Eintritt in den Ruhestand), und die einzelnen Kategorien des Systems werden über die „Intelligenz" verfügen, für die betreffende Person jeweils maßgebliche Inhalte vorzuschlagen. Personen, die Verwaltungsfunktionen ausführen möchten, wird der Makler über das Portal alle Leistungen aus einer Hand anbieten können. Bestimmte Angebote können nach und nach weiter personalisiert werden, wenn aufgrund wiederholter Zugriffe individuelle Benutzerprofile erstellt werden. Die Regierung ist der Ansicht, das Privatleben der Benutzer werde respektiert, da die Benutzer ihre Zustimmung zur entsprechenden Nutzung und Speicherung ihrer Daten für die Bereitstellung des jeweiligen Angebots erteilen müssen. Die irische Datenschutzbehörde hat dieses Modell vorbehaltlich strenger Datenschutzbestimmungen in Bezug auf die Zustimmungspflicht und die Nutzung der Daten zu bestimmten Zwecken genehmigt.

Die niederländische Datenschutzbehörde hat dieses Thema ebenfalls diskutiert und auf die Auswirkungen der operativen Unterscheidung zwischen „*Front Office*" und „*Back Office*", d.h. zwischen Angeboten mit unmittelbarem Bürgerkontakt (Schalter und Bürgerbüros) einerseits und Angeboten, bei denen Daten verwaltet werden, andererseits, hingewiesen. Verwaltungsangebote im „Front Office"-Bereich erfassen alle Datentypen, die zur Erbringung der von den Bürgern benötigten Leistungen erforderlich sind, während Verwaltungsangebote im „Back Office"-Bereich diese Daten nutzen, um sich unter Berücksichtigung der in Anspruch genommenen Angebote ein Bild von der Situation der Bürger zu machen; entsprechend können die Verwaltungen über eine einzige Anlaufstelle unterschiedliche Leistungen anbieten. Die Verwaltung beschränkt sich mehr und mehr auf diese Organisationsstruktur, für die die Begriffe „Portal" und „zentrale Anlaufstelle" bezeichnend sind. In ihrem Jahresbericht hat die niederländische Datenschutzbehörde auf die Tatsache verwiesen, dass Verwaltungen unter diesen Umständen die jeweiligen Zuständigkeiten der verschiedenen betroffenen Verwaltungen entsprechend den jeweils verarbeiteten Daten definieren müssen, um die rechtswidrige Nutzung und Weitergabe von Bürgerdaten in Verbindung mit „Back Office"-Angeboten zu verhindern.

2. Einbeziehung privater externer Provider, die personenbezogene Benutzerdaten speichern können bzw. auf personenbezogene Benutzerdaten Zugriff haben

Die Nähe zwischen der elektronischen Verwaltung und kommerziellen Online-Verfahren sowie entsprechend die Möglichkeit des Angebots von Verfahren der Online-Verwaltung durch private Unternehmen zwingen dazu, verschiedene Fragen bezüglich der technischen Gestaltung der elektronischen Verwaltung zu prüfen: Können private Unternehmen die gleichberechtigte Behandlung der Bürger in den öffentlichen Verfahren gewährleisten? Wie werden die Verfahren abgerechnet? Bedeutet dies, dass bestimmte Verfahren der Online-Verwaltung kostenpflichtig sind? usw.

In den verschiedenen Ländern der Europäischen Union wurden diese Fragen unterschiedlich beantwortet.

Deutschland, Italien, Spanien, die Niederlande, Schweden und Norwegen haben sich entschieden, von einer Einbeziehung privater Provider abzusehen, wenn diese auf personenbezogene Daten der Benutzer zugreifen können. In den meisten Ländern und insbesondere in Spanien müssen die öffentlichen Stellen allerdings z.B. bei der Entwicklung von Produkten oder Portalen auf private externe Provider zurückgreifen. In Spanien sind private Betreiber darüber hinaus aufgerufen, an der Durchführung von Prüfplänen in Verbindung mit der Entwicklung von Portalkonzepten mitzuarbeiten.

Die entgegengesetzte Haltung vertreten Belgien, Dänemark, Frankreich (nur gelegentlich), Finnland und Österreich. Dort können geeignete private Provider eine Zulassung beantragen; dazu müssen die Provider allerdings nachgewiesen haben, dass sie die erforderlichen Sicherheitsgarantien insbesondere hinsichtlich des Datenschutzes übernehmen können. Portugal und das Vereinigte Königreich zeigten sich gleichgültig; in diesem Rahmen bestehen jedoch keine grundsätzlichen Einwendungen gegen eine Einbeziehung privater externer Provider.

In Verbindung mit Projekten der elektronischen Verwaltung wollte keines der Länder den Passport-Dienst von Microsoft einführen; manchen Datenschutzbehörden lagen keine spezifischen Informationen zu dieser Frage vor.

3. Meinung der Datenschutzbehörden zu diesen Themen und Reaktionen der Regierungen

Die Datenschutzbehörden haben die Fragen betreffend die Einrichtung eines Portals in ihren jeweiligen Ländern nicht immer beantwortet, insbesondere weil die bestehenden Projekte nicht in jedem Fall eine Speicherung der personenbezogenen Daten in den Portalen vorsehen.

In den Ländern, in denen im Portal personenbezogene Daten verarbeitet werden, bestanden die Datenschutzbehörden dagegen auf der Tatsache, dass eine Einbeziehung externer Provider erst dann in Betracht gezogen werden könne, wenn die spezifischen Garantien umgesetzt werden. Abhängig von den Empfehlungen unterschiedlicher Behörden werden folgende Garantien gefordert: geeignete Verträge mit datenverarbeitenden Unternehmen, genau definierte Aufgaben der externen privaten Provider, Bestimmung der Sicherheitsbedingungen (geschützte und vollständig automatisierte Umgebung), Erfüllung bestimmter juristischer Anforderungen an die privaten externen Provider (Zulassung) einschließlich insbesondere des Verbots der Verwendung der ihnen anvertrauten Daten zu sonstigen Zwecken sowie des Verbots der Offenlegung der Daten, exakte Bestimmung der registrierten Daten, mögliche Einrichtung eines Prüfausschusses usw.

D. NATIONALE SYSTEME ZUR IDENTIFIZIERUNG VON EINZELPERSONEN (VERWENDUNG EINDEUTIGER PERSONENBEZOGENER ODER SEKTORBEZOGENER KENNZIFFERN FÜR DEN ZUGRIFF AUF BESTIMMTE ANGEBOTE DER ONLINE-VERWALTUNG)

Zunächst einmal ist festzuhalten, dass bis heute nur Belgien, Dänemark, Spanien, Finnland, Irland, Italien, Luxemburg, Norwegen und Schweden eine personenbezogene und eine allgemeine Kennziffer auf nationaler Ebene verwenden. In anderen Ländern, insbesondere in Österreich, laufen Projekte zur Entwicklung dieser Kennziffern; die Kennziffern werden jedoch nur als verborgene Ausgangsnummern zur Erzeugung

sektorbezogener Kennziffern genutzt (siehe unten). In Dänemark, Belgien und Spanien wird die personenbezogene Kennziffer neben sektorbezogenen Kennziffern verwendet. In den übrigen Ländern werden ausschließlich sektorbezogene Kennziffern eingesetzt: in Deutschland die Sozialversicherungsnummer und die Ausweisnummer, in Frankreich und in Portugal im Wesentlichen die Sozialversicherungsnummer und in Griechenland und in den Niederlanden besonders die Sozialsteuernummer. In Ländern wie Deutschland und Portugal wird die Verwendung einer personenbezogenen Kennziffer als verfassungswidrig betrachtet.

Die Entwicklung der elektronischen Verwaltung bietet gelegentlich die Möglichkeit einer Neukonzeption dieses Systems der Kennziffern bzw. die Möglichkeit der Erweiterung des Spektrums sektorbezogener Kennziffern. Zurzeit erklären nur Portugal und Österreich, dass diese Entwicklungen mit einer Umgestaltung des nationalen Systems der Personenidentifizierung einhergehen.

1. Der allgemeine Trend geht dahin, für den Zugang zu den Verfahren der Online-Verwaltung bereits definierte personenbezogene Kennziffern (Belgien, Dänemark, Spanien, Irland) oder sektorbezogene Kennziffern (Frankreich, Niederlande, Portugal, Italien) zu verwenden. In manchen Ländern, in denen keine eindeutigen Kennziffern verwendet werden, wird die Ansicht vertreten, die Einrichtung eines personalisierten Portals durch die Verwaltung dürfe nicht zum Anlass genommen werden, eine eindeutige Kennziffer einzuführen (insbesondere Frankreich). In Österreich besteht in dieser Hinsicht eine besondere Situation: Dort soll eine eindeutige Kennziffer (die ZMR-Zahl (Melderegisterzahl)) eingeführt werden, die außerhalb des Melderegisters nicht gespeichert werden darf und ausschließlich zur Erzeugung sektorbezogener Kennziffern mittels eines besonders geschützten Verfahrens verwendet wird. Öffentliche Stellen sind nicht befugt, die Kennziffern eines Sektors außerhalb ihres jeweiligen Aufgabenbereichs zu speichern.

2. In manchen Ländern wurden bzw. werden noch immer Projekte zur Erweiterung sektorbezogener Kennziffern für den Zugang zu Verfahren der Online-Verwaltung geprüft. Ein Projekt zur Verallgemeinerung der Sozialversicherungs- und Steuernummer in den Niederlanden wurde infolge einer nachteiligen Bewertung durch die Datenschutzbehörde von der Regierung aufgegeben. Derzeit besteht ein entsprechendes Projekt nur in Italien; dort geht man davon aus, dass die Steuernummer hin zu einer personenbezogenen Kennziffer für den Zugang zu bestimmten Verfahren der Online-Verwaltung verallgemeinert wird. In Irland wurde die PPSN („*Personal Public Service Number*“) als gesetzlich vorgeschriebene Kennziffer für Zugriffe auf öffentliche Angebote eingeführt; nach den geltenden Rechtsvorschriften kann diese Kennziffer für Angebote der Finanzbehörden und der Sozialversicherungen sowie für die Angebote sonstiger überregionaler oder lokaler Behörden genutzt werden.

3. In Italien wurde anfänglich über das Risiko der Generalisierung einer de facto sektorbezogenen Kennziffer (in diesem Fall die italienische Steuernummer) im Anschluss an die Aufnahme in einen elektronischen Ausweis diskutiert: Die italienische Datenschutzbehörde erinnert die Regierung daran, dass es gemäß Artikel 8 Ziffer 7 der Richtlinie 95/46 über die Einrichtung einer personenbezogenen Kennziffer ratsam sei, die Bedingungen festzulegen, unter

denen die Kennziffer verwendet werde. Die italienische Regierung versicherte der italienischen Datenschutzbehörde, dass die Regierung diese Haltung berücksichtigen werde; bislang wurde die Situation aber noch nicht endgültig geklärt.

4. In Irland darf eine einheitliche Kennziffer verwendet werden; eine entsprechende Entwicklung wird in Belgien erwartet. In Belgien ist die Verwendung der nationalen Registernummer (und in der Regel für Personen, denen keine Nummer im nationalen Register zugewiesen wurde, die Verwendung der Sozialversicherungsnummer) als eindeutige Kennziffer von nun an in allen Informationssystemen der öffentlichen Stellen zwingend vorgeschrieben. Die Datenschutzbehörde muss umgehend ihre Haltung in dieser Frage darlegen.

5. Ausschließlich sektorbezogene Kennziffern werden in Deutschland, in Portugal, im Vereinigten Königreich und in Frankreich eingesetzt. Die sektorbezogenen Kennziffern werden ausschließlich für den ursprünglich vorgesehenen Zweck genutzt.

6. Mit der gleichen Logik der Vermeidung von Risiken durch den Austausch von Daten haben andere Datenschutzbehörden die Einführung abgeleiteter sektorbezogener Kennziffern beantragt oder vorschlagen (insbesondere in den Niederlanden, wo ein vorläufiger Entwurf der Regierung entsprechend geändert wurde, und in Österreich, wo die (verborgene) eindeutige Kennziffer in Verbindung mit der elektronischen Signatur in einer Sonderfunktion (der so genannten „Bürgerkarte") zur Sicherung des Online-Zugangs zu sämtlichen Anwendungen der elektronischen Verwaltung sowie sogar zu besonders strukturierten Online-Anwendungen im privaten Sektor genutzt wird.

7. Sonderfälle:

   - In Finnland wird ein Projekt zur Revision der Systeme zur Personenidentifizierung in Verbindung mit der elektronischen Verwaltung verfolgt; dieses Projekt strebt die Verwendung einer eindeutigen Kennziffer an, die speziell für die Zwecke der elektronischen Identifizierung beim nationalen Bevölkerungsregister erzeugt wird. Es wird nicht davon ausgegangen, dass diese Kennziffer für den Zugang zu Verfahren der Online-Verwaltung verwendet werden soll. Für diese Zwecke sollte die bereits verwendete personenbezogene Kennziffer (die Sozialversicherungsnummer) genutzt werden.
   - In Belgien war die Entwicklung der elektronischen Verwaltung Anlass zur Erzeugung einer eindeutigen Kennziffer für Unternehmen: Die derzeit verwendete Umsatzsteueridentifikationsnummer (unter Einbeziehung der nicht umsatzsteuerpflichtigen Unternehmen und Organisationen) wird zu einer eindeutigen Kennziffer für alle Unternehmen und Organisationen entwickelt. Diese Kennziffer wird dann alle sonstigen spezifischen Kennziffern ersetzen und soll in allen Informationssystemen der öffentlichen Stellen als eindeutige Kennziffer für Unternehmen und Organisationen verwendet werden.

E. DURCH DIE ENTWICKLUNG DER ELEKTRONISCHEN VERWALTUNG BEDINGTER DATENAUSTAUSCH

Die britische Datenschutzbehörde brachte besondere Bedenken dahingehend zum Ausdruck, dass die Entwicklung der elektronischen Verwaltung nicht zur Vertuschung eines allgemeinen Datenaustauschs zwischen den öffentlichen Informationsdatenbanken und eines zunehmenden Austauschs personenbezogener Daten zwischen den Verwaltungen dienen dürfe. Außerdem stellt die CNIL ihre allgemeine Grundhaltung dar, nach der jeglicher allgemeiner Datenaustausch abgelehnt wird. Die CNIL betont diese Position anlässlich der Anhörungen, die von den Autoren eines auf Antrag der Regierung geschriebenen Berichts über elektronische Verwaltung und den Schutz personenbezogener Daten organisiert wurden. Nach der Übergabe dieses Berichts an die Regierung wurde eine öffentliche Diskussion der beim Erstellen des Berichts erkannten wesentlichen Punkte eingeleitet. Eine der wichtigsten Schlussfolgerungen dieser öffentlichen Entscheidungen, die vollständig im Einklang mit der Grundhaltung der CNIL steht, besteht in der Überzeugung, dass die elektronische Verwaltung nicht zu einer verstärkten Überwachung von Einzelpersonen führen solle, die in erster Linie auf den Austausch der Daten zurückzuführen wäre.

In Deutschland ist außerdem hervorzuheben, dass das Verfassungsgericht gerade im Hinblick auf den Datenaustausch weiterhin das bekannte Prinzip des Rechts auf informationelle Selbstbestimmung der Bürger vertritt. Dieses Recht besteht darin, dass jeder einzelne Bürger über die Weitergabe und die Verwendung seiner Daten an Dritte bzw. durch Dritte entscheiden kann. Die Anerkennung dieses Rechts - soweit dieses Recht nicht einem absoluten Verbot des Datenaustauschs gleichkommt - begrenzt zumindest viele Möglichkeiten, die ansonsten gegeben wären.

Wenn Länder angaben, dass ein Datenaustausch beabsichtigt sei, war die wesentliche Motivation für diese Entwicklung der Wunsch, die bestehenden Verfahren zu vereinfachen. Diese Motivation besteht bei den Unternehmen sowie bei den Bürgern und bei letzteren insbesondere in Verbindung mit Umzugsmeldungen. Außerdem wurde als Ziel die Betrugsbekämpfung genannt (insbesondere in Irland und im Vereinigten Königreich).

Zurzeit ist dieser Datenaustausch im Allgemeinen nicht definiert, bzw. Definitionen werden noch entwickelt. Welche Bereiche betroffen sind, hängt von den jeweiligen nationalen Anliegen ab: in Spanien und in Finnland insbesondere der Gesundheitssektor, in Belgien die Gestaltung der Beziehungen zwischen Verwaltungen und Unternehmen, in Italien die Indizierung öffentlicher Dateien und in Spanien die Einführung von Informationsverfahren in den Behörden (insbesondere über das so genannte „Einheitliche Fenster“ (*Ventanilla Única 2*), das während der Verfahren ausgehend von einem Austausch der vorhandenen Dokumente eine Koordinierung zwischen unterschiedlichen Verwaltungsabteilungen ermöglicht).

Mehrere Datenschutzbehörden sind an Arbeitsgruppen beteiligt, in denen diese Fragen untersucht werden (z.B. in den Niederlanden oder in Finnland); andere Datenschutzbehörden (z.B. die CNIL) beschäftigen sich mit diesen Fragen, da sie die Verarbeitung personenbezogener Daten im öffentlichen Sektor im Vorfeld zu prüfen haben.

In Verbindung mit diesen Projekten stellen sich in allen betroffenen Ländern regelmäßig die gleichen Fragen:

- Auf juristischer Ebene wird der Datenaustausch im Rahmen einer gesetzlichen Autorisierung (Frankreich) oder im Rahmen von Bestimmungen behandelt, welche die Zustimmung der betreffenden Personen vorsehen. In Spanien z.B. ist die Datenschutzbehörde der Ansicht, dass das Regulierungsprojekt zur Förderung der elektronischen Verwaltung die Anforderungen des allgemeinen Datenschutzrechts erfüllt, da die Zustimmung der betroffenen Personen vor dem elektronischen Transfer der Daten zwischen den Verwaltungen vorgeschrieben ist. Diese Regelung wurde durch das Königliche Dekret vom 28. Februar 2003 betreffend die Verordnung zu telematischen Registern, Notifizierungen, Zertifikaten und Übertragungen angenommen. Außerdem beschreibt das Dekret die in Verbindung mit diesen Systemen einzusetzenden Verfahren, insbesondere im Zusammenhang mit Mitteilungen an die Bürger oder mit dem Informationsaustausch mit den Behörden. Für den Informationsaustausch mit den Behörden ist die vorherige Zustimmung zur Übertragung der jeweiligen Daten erforderlich. Außerdem enthält das Dekret eine Bestimmung, welche die Behörden zur Einhaltung des Datenschutzgesetzes verpflichtet.
- Hinsichtlich des Datenschutzes hielten die Länder insbesondere die Datenqualität, die Legitimität der Verarbeitung und die Aufklärung der betroffenen Personen sowie die umgesetzte Sicherheitsstufe für maßgeblich.

Die Fragen in Verbindung mit der Notwendigkeit und den allgemeinen Bedingungen der Umsetzung des Datenaustauschs wurden besonders im Vereinigten Königreich untersucht; Anlass der Untersuchung war die Veröffentlichung eines im Jahre 2002 von der britischen Regierung in Auftrag gegebenen Berichts der „*Performance and Innovation Unit*“ (einer dem Kern der britischen Regierung angehörenden Einrichtung zur strategischen Überprüfung, die nun als *Strategy Unit* bezeichnet wird). Unter dem Titel „*Privacy and data sharing: the way forward for public services*“ beleuchtet dieser Bericht den Aspekt des durch die Entwicklung der elektronischen Verwaltung offenbar verstärkten Datenaustauschs und der diesbezüglichen Erwartungen der Bürger; gleichzeitig betont der Bericht jedoch die gleichwertige Bedeutung der Erwartungen der Bürger in Bezug auf den Schutz ihres Privatlebens. Daher ist die Betonung der Erwartungen hinsichtlich des Datenschutzes wichtig, um das erforderliche Gleichgewicht zwischen dem Bedürfnis nach einem Austausch des Datenmaterials (und der zu erwartenden Verbesserungen der Angebote seitens der Verwaltung) und dem Schutz der Benutzer bei der Verarbeitung ihrer personenbezogenen Daten herzustellen. Die Herstellung dieses Gleichgewichts setzt die Analyse der folgenden Fragen voraus:

- Welche Vorteile sind von der Verwendung der Daten und dem Austausch der Daten vor dem Hintergrund der Zielsetzungen der Regierung zu erwarten?
- Bestehen alternative Ansätze zur Erreichung des gleichen Ziels?
- Welche Risiken und welche Kosten gehen mit dem Austausch der Daten einher?
- Welche Garantien könnten erforderlich sein, um diese Risiken in den Griff zu bekommen (z.B. PETs)?
- Zum Abschluss der Analyse ist zu klären, ob sich Vorteile und Risiken des beabsichtigten Datenaustauschs die Waage halten.

Eines der wesentlichen Anliegen des Berichts besteht nicht zuletzt darin, daran zu erinnern, dass der Datenaustausch keine unvermeidliche Bedingung für die Verbesserung der Angebote der Verwaltung darstellt.

F. ELEKTRONISCHE SIGNATUR UND PKI (PUBLIC KEY INFRASTRUCTURE)

Die meisten Vertretungen geben an, dass die Beteiligung privater Betreiber („Zertifizierungsdiensteanbieter") im Rahmen der Einführung von Systemen zur Verwendung elektronischer Signaturen in Verbindung mit bestimmten Verfahren der Online-Verwaltung in den betreffenden Ländern zulässig sei bzw. wäre. In diesen Fällen sind die Geschäftsbedingungen des Zertifizierungsdiensteanbieters rechtsverbindlich gefasst (z.B. in Form von Vereinbarungen). Diese Fragen wurden häufig bei der Umsetzung der Richtlinie zu elektronischen Signaturen in nationales Recht gelöst.

In den übrigen Fällen ist eine Einbeziehung privater externer Anbieter ausgeschlossen, weil nur der Staat diese Rolle übernehmen darf (Deutschland, Spanien). In Frankreich gilt grundsätzlich, dass private externe Anbieter bislang nur die Zertifizierung von Online-Umsatzsteuererklärungen übernehmen. Ansonsten fungiert der Staat als Zertifizierungsbehörde.

Im Allgemeinen wird betont, dass Systeme mit elektronischen Signaturen derzeit nicht sehr verbreitet seien, da entweder ein geeigneter juristischer Rahmen fehle oder da die Systeme noch zu teuer oder zu komplex seien. Entsprechend unterstreicht die CNIL, dass die systematische Einbeziehung dieser Prozesse keine Voraussetzung für die Umsetzung von Verfahren der Online-Verwaltung darstellen könne. Angesichts der aktuellen Rechtslage sowie des Standes der Technik und der Marktsituation der *Public Key Infrastructures* wäre die Umsetzung dieser Anforderungen verfrüht. Vielmehr wird darauf hingewiesen, dass bestimmte Verwaltungsverfahren deshalb noch nicht online angeboten werden, weil diese Verfahren die Einrichtung eines elektronischen Signatur- und Verschlüsselungssystems erfordern würden. Daher haben mit wenigen Ausnahmen viele Verwaltungen noch keinerlei öffentlich zugängliches allgemeines Verfahren in Verbindung mit einem System zur Verarbeitung elektronischer Signaturen eingerichtet. Eine Ausnahme bildet z.B. Dänemark. Dort wurden bereits Systeme zur Nutzung elektronischer Signaturen entwickelt. Die elektronischen Signaturen werden den Bürgern kostenlos zur Verfügung gestellt, und viele Internet-Portale werden für die Abwicklung von Diensten der elektronischen Verwaltung ausgerüstet.

Die Anwendungsbereiche für diese Systeme sind je nach Land Ausdruck unterschiedlicher Prioritäten: z.B. Steuerwesen und Sozialsektor (Frankreich) oder Volkszählungen (Finnland). In den meisten Fällen werden diese Systeme von Einzelpersonen, Unternehmen und Vertretern der Verwaltung gleichermaßen genutzt. Manchmal haben zunächst Einzelpersonen Zugriff (Deutschland), manchmal werden diese Systeme zunächst für die Mitarbeiter, die Unternehmen und die Server eingesetzt und sind folglich nicht vorrangig für die Bevölkerung verfügbar (Dänemark), und gelegentlich nutzen zunächst Vertreter der Verwaltung die Systeme (Norwegen). Hinsichtlich der Vertreter der Verwaltung wurde folgende Unterscheidung vorgenommen: In Verbindung mit Vertretern der öffentlichen Hand ist weniger wichtig, dass die elektronische Signatur die jeweilige Einzelperson ausweist; vielmehr soll die Signatur Aufschluss darüber geben, ob die unterzeichnende Person über die erforderliche Entscheidungskompetenz bzw. über die erforderliche Kompetenz zur Veranlassung der jeweiligen Aktion verfügt.

Die Datenschutzbehörden konnten den öffentlichen Stellen bei verschiedenen Gelegenheiten ihre Standpunkte mitteilen. Manchmal wurden die Behörden bei der Verabschiedung von Gesetzen und Regulierungsbestimmungen zur Gestaltung von Prozessen mit elektronischen Signaturen angehört. In anderen Fällen nahmen die

Behörden Stellung, nachdem sie aufgefordert wurden, bestimmte Anwendungen zu überprüfen.

Die allgemeine Haltung der Datenschutzbehörden gegenüber Systemen mit elektronischer Signatur ist positiv, da diese Systeme als Mechanismen verstanden werden, welche den Schutz personenbezogener Daten verbessern könnten. Einige Behörden haben jedoch die Wichtigkeit der Einbeziehung von Fragen des Datenschutzes in die Entwicklung dieser Mechanismen betont. Insbesondere wurde empfohlen, den Benutzern eindeutige Informationen der Zertifizierungsdiensteanbieter zur Weitergabe der Daten zukommen zu lassen, welche die Rechtsvorschriften betreffend die Weitergabe personenbezogener Daten erfüllen. Die österreichische Datenschutzbehörde betrachtet die eindeutige Identifizierung von Personen, die online auf personenbezogene Daten zugreifen möchten, als wesentlichen Beitrag zum Datenschutz in der elektronischen Verwaltung.

G. ELEKTRONISCHE AUSWEISE

1. Zurzeit sind die elektronischen Ausweiskarten der Bürger in den europäischen Ländern meist sektorbezogene Karten. In erster Linie ist dies die Sozialversicherungskarte, die manchmal langfristig mit einer Krankenversicherungskarte kombiniert werden soll. Diese sektorbezogene Karte besteht manchmal parallel neben einer allgemeinen Ausweiskarte (besonders in Belgien und in Finnland).

2. Letztendlich sollte die allgemeine Karte in ebenso vielen Ländern eingesetzt werden wie in Ländern, in denen nur sektorbezogene Karten verwendet werden. Allgemeine elektronische Ausweise werden zurzeit nur in Belgien, Italien und Finnland ausgehändigt; in Deutschland, in Schweden, in Frankreich, in Spanien und im Vereinigten Königreich (dort als so genannte „Berechtigungskarten“) sollen allgemeine elektronische Ausweise eingeführt werden. Diese Karte soll nicht zur Personenüberprüfung genutzt werden, sondern nur als Ausweis für die Personen dienen, die auf bestimmte Angebote der Online-Verwaltung zugreifen möchten; darüber hinaus soll diese Karte als Sozialversicherungskarte eingesetzt werden. Auch in Portugal wird ein Projekt zur Einführung einer individuellen Karte durchgeführt. Ein Ziel könnte darin bestehen, verschiedene Datentypen auf einer einzelnen Karte so unter verschiedenen Kennziffern zusammenzufassen, dass die Verwaltungen nur auf die Daten zugreifen können, die sie jeweils tatsächlich betreffen. Eine Studie zur technischen Machbarkeit dieser Karte wird derzeit durchgeführt. Die portugiesische Datenschutzbehörde wünscht, über die entsprechenden Fortschritte informiert zu werden, um die Berücksichtigung der Rechtsvorschriften sicherzustellen, nach denen die Zuordnung einer einzigen Kennziffer in Portugal verboten ist.

3. Über die umfangreichsten Erfahrungen mit elektronischen Ausweisen verfügen derzeit Italien und Finnland.

   - In Finnland besteht die elektronische Ausweiskarte aus einem Ausweis mit einem Foto des Inhabers und einem Chip, auf dem das Authentifizierungszertifikat des Inhabers, das für Anwendungen in Verbindung mit elektronischen Signaturen erforderliche Anerkennungszertifikat und das Zertifikat des Zentrums für die Durchführung von Volkszählungen (das *Population Register Centre*), das die „E-Nummer“

der betreffenden Personen übermittelt, gespeichert sind. Diese allgemeine Nummer wird vorwiegend im Rahmen kommerzieller Transaktionen genutzt. Die Karte enthält keine sonstigen Informationen in Verbindung mit der (nach der Geburt zugewiesenen) allgemeinen Kennziffer der betreffenden Person (weder die Anschrift noch das Geburtsdatum). Die erforderliche Sicherheit wird durch eine Persönliche Identifizierungsnummer (PIN) hergestellt, mit der die Benutzer auch auf Informationsnetze wie z.B. das Internet zugreifen können. Über ihre Funktion als Ausweis (sowie als Reisepass oder Führerschein) hinaus kann diese Karte auch zur elektronischen Identifizierung und für elektronische Signaturen genutzt werden. Die Karte kann in Verbindung mit kommerziellen Transaktionen eingesetzt, aber auch in Verwaltungsprozessen verwendet werden. Mit der Karte sowie mit einer speziell für diesen Zweck vom *Population Register Centre* und von der finnischen Post entwickelten Applikation können z.B. Adressänderungen online validiert werden. Im November 2002 hat die Regierung außerdem vorgeschlagen, diesen Ausweis mit der Sozialversicherungskarte zu verbinden. Auf Anfrage des Ombudsmanns für den Datenschutz wurde in dem Projekt erklärt, dass die Bürger selbst bestimmen können, ob Sozialversicherungs- und Gesundheitsdaten in die Karte aufgenommen werden.

Zurzeit kostet die Karte € 29 bei einer Gültigkeitsdauer von 3 Jahren; die Gebühren sollen auf € 40 angehoben werden; gleichzeitig soll die Gültigkeitsdauer auf 5 Jahre erhöht werden. Die Karte wird nicht ausschließlich finnischen Bürgern ausgehändigt: Auch Ausländer, die sich gültig ausgewiesen haben und über einen ständigen Wohnsitz in Finnland verfügen, können eine Karte erhalten.

Die Karten werden von den örtlichen Polizeidienststellen gegen Vorlage des Ausweises, des Reisepasses oder eines Führerscheins ausgehändigt. Das *Population Register Centre*, das innerhalb der finnischen Verwaltung als Zertifizierungsdiensteanbieter fungiert, stellt die erforderlichen Zertifikate für die elektronische Identifizierung aus. Außer der Karte wird noch ein kleines Kartenlesegerät benötigt, das die Benutzer zu Hause verwahren müssen. Die Identifizierung wird letztlich jedoch über ein mobiles Gerät wie z.B. ein mit einem besonderen Chip ausgerüstetes Mobiltelefon erfolgen können. Ein System zur Meldung gestohlener oder verlorener Karten ist rund um die Uhr erreichbar.

Der finnische Ausweis hat die Erwartungen nicht erfüllt. Bislang haben nur 13 000 Finnen den Ausweis erhalten. Als wesentliche Faktoren für diese zögernde Akzeptanz werden genannt, dass die Karte nicht kostenlos ausgestellt wird, dass die Benutzer für kommerzielle Transaktionen über das Internet Smart-Card-Lesegeräte zu Hause besitzen müssen und dass die Vorzüge des Systems verhältnismäßig unbestimmt wahrgenommen werden. Und da die Karte nur fakultativ ausgestellt wird, sind die Finnen mehrheitlich bei den herkömmlichen Ausweispapieren geblieben.

- Die in Italien verwendete elektronische Ausweiskarte soll die Ausweispapiere ersetzen und ist daher für alle Bürger zwingend erforderlich. Das derzeitige Projekt sieht vor, dass die Karte nicht auf die Funktion eines reinen Ausweises beschränkt ist, sondern gleichzeitig als Nachweis der Staatsangehörigkeit und des Rechts auf Freizügigkeit innerhalb der

Europäischen Union dient; darüber hinaus würde die italienische Ausweiskarte den Zugang zu den nationalen und lokalen öffentlichen Stellen ermöglichen, eine Funktion zur Übertragung elektronischer Signaturen beinhalten und den Bürgern die Möglichkeit der Online-Abstimmung bieten. Ergänzend könnten Funktionen wie z.B. die Möglichkeit der Online-Terminvereinbarung mit Ärzten angeboten werden.

Diese Karte kann auch für Minderjährige ausgestellt werden und beinhaltet außer den Identifizierungsdaten auch die Steuernummer der jeweiligen Person. Langfristig wird die Karte Fingerabdrücke und Gesundheitsdaten (außer der DNA) enthalten (soweit vom jeweiligen Inhaber zur Registrierung freigegeben). Diese Anforderung der vorherigen Datenfreigabe durch den jeweiligen Inhaber wurde auf Betreiben der italienischen Datenschutzbehörden vorgeschrieben. Die Regierung beabsichtigt, die Verwendung der Karte im Internet durch die Einrichtung öffentlicher Terminals in Bars, Restaurants und Läden zu fördern; die elektronische Ausweiskarte dient dann zur Online-Identifizierung. Ein weiteres Ziel dieser Aktion besteht darin, dass die Betreiber von Ladengeschäften die Funktion von „Schaltern“ übernehmen; dadurch könnten die Verwaltungen langfristig die mit den entsprechenden Verwaltungsleistungen verbundenen Kosten senken.

Als problematisch an der Umsetzung dieses Projektes sieht das italienische Innenministerium unter anderem die logische Zusammenfassung der Behörden bei der Ausstellung der Karte sowie die Garantie der Unabhängigkeit der Kommunen bei der Umsetzung ihrer Online-Angebote für die Bürger und die Umsetzung eines Sicherheitskonzeptes im Hinblick auf die eigentliche Karte sowie für den gesamten Lebenszyklus der Karte. Dieses Sicherheitskonzept besteht z.B. aus der Beschreibung eines komplexen Prozesses für Produktion, Initialisierung, Aktivierung und Ausstellung der Karte; die Ausstellung sollte durch die örtlichen Behörden erfolgen, denen die Aufgabe zukommt, die personenbezogenen Daten (einschließlich eines Fotos) zu erfassen und auf den Karten zu registrieren.

Die Karte nutzt zwei Technologien auf einem herkömmlichen Kunststoff-Trägermaterial: einen 16-KB-Mikroprozessor und einen Magnetstreifen. Auf der Kunststoffkarte befindet sich ein sichtbares Foto; außerdem sind auf der Karte Name, Vorname, Geschlecht, Datum und Geburtsort der jeweiligen Person sowie eine eindeutige Kennziffer angegeben. Auf der Rückseite sind Adresse und Steuernummer der Person sowie die Gültigkeitsdauer der Karte vermerkt und die beiden technischen Elemente (Mikroprozessor und Magnetstreifen) untergebracht. Das Hologramm auf dem Magnetstreifen enthält den Fingerabdruck und die Unterschrift der Person.

Beide Technologien haben ihre jeweils spezifische Funktion: Auf dem Magnetstreifen sind die Ausweisinformationen untergebracht, während die leistungsbezogenen Funktionen über den Mikroprozessor abgewickelt werden. Der Mikroprozessor ermöglicht eine zuverlässige Identifizierung und eine Authentifizierung mit Hilfe symmetrischer und asymmetrischer Schlüssel. Auf einer Karte können bis zu 16 Schlüssel gespeichert werden.

4. Bei Projekten für allgemeine elektronische Ausweiskarten werden die Funktionen der Karten in der Regel zusammengefasst.

   In erster Linie dient die Karte als Ausweis der betreffenden Person.

   1. Außerdem wird regelrecht systematisch beabsichtigt, die Karte zur Einrichtung von Verfahren der Online-Verwaltung (außer - nach derzeitigem Kenntnisstand - in Deutschland), zur individuellen Identifizierung und zur Authentifizierung im Rahmen elektronischer Handelsgeschäfte (in Spanien noch nicht definiert) einzusetzen.
   2. Die Funktion der elektronischen Signatur wird für Verfahren der Online-Verwaltung ebenso wie im elektronischen Handel (in Spanien allerdings ebenfalls noch nicht definiert) systematisch angestrebt.
   3. Die Karten haben die Funktion einer Kreditkarte nur in Deutschland, Italien, Österreich, Portugal und Schweden.
   4. Die Funktion einer „Krankenversicherungskarte“ wird nur in Deutschland und in Finnland ausdrücklich beibehalten; in Portugal, Italien und Österreich hingegen wird diese Möglichkeit geprüft.
   5. Als „Sozialversicherungskarte“ soll die Karte nur in Deutschland und in Finnland beibehalten werden. In den übrigen Ländern übernehmen diese Funktion häufig sektorbezogene Karten.
   6. Außerdem könnten diese Karten in Deutschland, in Italien und in den Niederlanden sowie u.U. in Portugal und in Schweden als Stimmkarten eingesetzt werden.

5. Die meisten europäischen Datenschutzbehörden wurden zu diesen Punkten angehört. Einige Datenschutzbehörden äußerten sich zustimmend zu den Projekten der öffentlichen Stellen (Finnland, Schweden); andere Behörden diskutieren derzeit noch bereits bestehende Projekte. Manche Behörden vertreten eine von der für das jeweilige Projekt zuständigen Verwaltung abweichende Haltung (Italien, Niederlande). In jedem Fall werden verschiedene Punkte als möglicherweise problematisch empfunden:

   1. Bestimmung der Art der auf der Karte registrierten Daten,
   2. Bestimmung der Verfahren zur Datenverarbeitung,
   3. Bestimmung der Organisationen, denen Zugriff auf die verschiedenen Informationskategorien gewährt werden soll,
   4. Wahrung der Persönlichkeitsrechte,
   5. Bestimmung der Verwaltungen, die über die Art der auf den elektronischen Karten registrierten Daten entscheiden können sollen,
   6. mögliche Nutzung der elektronischen Ausweise für kommerzielle Zwecke (Online-Zahlungen, elektronische Brieftasche usw.),
   7. getroffene Sicherheitsvorkehrungen (wobei Italien betont, dass bislang weltweit nur ein Unternehmen Lösungen anbieten könne, die die technologischen Anforderungen des Projektes erfüllen würden),
   8. zentrale Speicherung von Gesundheits- und Biometriedaten (Fingerabdrücke).

H. KONTROLLE DER BENUTZER ÜBER DIE EIGENEN PERSONENBEZOGENEN DATEN

Dieser Punkt wird in den einzelnen Ländern der Europäischen Union unterschiedlich gesehen. Die britische Datenschutzbehörde erklärt, der Wunsch, kohärente und

praktische Angebote für die Benutzer einzurichten und das Bestreben, die Quellen personenbezogener Informationen zu kombinieren (unter Umständen unter Verletzung der Datenschutzbestimmungen), könne zu Spannungen innerhalb der Behörde führen. Die Kontrolle der jeweils eigenen personenbezogenen Daten durch die Bürger ist also der wesentliche Konfliktpunkt. Bei der Durchsicht der Antworten der Datenschutzbehörden sind in Verbindung mit diesen Fragen zwei wesentliche Tendenzen festzustellen:

Eine erste Tendenz, der sich mehrere Länder (Irland, Dänemark, Spanien, Finnland) im Allgemeinen mit der Zustimmung der Datenschutzbehörden ausdrücklich anschließen, besteht in der Ansicht, dass die Bürger ihre persönlichen Daten während der Verwaltungsverfahren jederzeit unter Kontrolle haben müssen und dass vor jeder Entscheidung der betroffenen Bürger eine Rückmeldung über den Datenaustausch erfolgen müsse. Aus dieser Tendenz folgt, dass der Datenaustausch zwischen den Verwaltungen auf dem Wege der Telematik der Zustimmung der betroffenen Personen bedürfen kann (z.B. Spanien und Irland). Andere Länder nehmen eine eher zögernde Haltung ein (Vereinigtes Königreich, Belgien). Die erstgenannte Tendenz kann darauf zurückzuführen sein, dass diese persönliche Kontrolle das Vertrauen bedingt, aus dem eine elektronische Verwaltung sowie die Glaubwürdigkeit einer elektronischen Verwaltung erst erwachsen können. In gleicher Weise gilt zunehmend: Je mehr die Bürger sich auf ihre Verwaltung verlassen, desto weniger muss diese Kontrolle ausgeübt werden.

Selbst wenn die Benutzer allerdings die Kontrolle über ihre Daten haben, sind auch die wesentlichen Grundsätze des Datenschutzes zu beachten. Um die Bedingung der fairen Datenerhebung zu erfüllen, empfiehlt die irische Datenschutzbehörde, als Ausgangsmaterial nicht die bereits von den Verwaltungen erfassten Daten zu verwenden, sondern den Bürgern die Möglichkeit zu bieten, die Einbeziehung ihrer Daten in dieses neue System ausdrücklich zu genehmigen und die Bürger über die Zwecke und Anwendungen dieser zentralen Datenbank zu informieren. Außerdem muss der Grundsatz der Datenqualität gewahrt werden; entsprechend sollten überflüssige oder unerhebliche Daten, die voraussichtlich nicht in legitimer und maßgeblicher Weise in Anwendungen der Behörden genutzt werden, nicht erfasst und nicht gespeichert werden. Die Bürger sollten frei entscheiden können, welche zusätzlichen Daten übermittelt werden sollen, um umfangreichere Angebote zu ermöglichen. Ebenso muss den Bürgern bereits bei der Erfassung der Daten der Umfang der möglichen Anwendungen ihrer Daten bewusst sein, und die Vertreter der Verwaltungen sollten eindeutig über die Formen der legitimen Nutzung der Daten informiert sein, die ihnen zur Verfügung stehen. Diese Informationen müssen daher hinreichend genau sein, damit die Bürger die möglichen Risiken und Folgen einer Übertragung ihrer Daten in vollem Umfang erfassen. Wenn diese Informationen fehlen würden, wäre die Zustimmung der betroffenen Personen eine Illusion, da für die Bürger kein berechtigter Grund bestünde, in Anbetracht des Arguments der vereinfachten Verwaltungsverfahren die Weitergabe ihrer Daten zu verweigern.

Darüber hinaus betonen mehrere Datenschutzbehörden, ein weiterer wesentlicher Aspekt bestehe darin, dass eine befriedigende Sicherheit der eingesetzten Anwendungen gewährleistet sein müsse. Und wie die Darstellung eines kürzlich aufgetretenen Falls durch die spanische Datenschutzbehörde belegt, ist dieser Aspekt keineswegs theoretisch. In diesem Fall hatte eine örtliche Behörde zwei Finanzbehörden mit der Umsetzung eines Verfahrens zur Beantragung von Wohnbescheinigungen beauftragt; die Wohnbescheinigungen sollten von den betreffenden Bürgern zur Beantragung von Fahrscheinermäßigungen für öffentliche Verkehrsmittel vorgelegt werden. Die

Finanzbehörden stellten diese Bescheinigungen über die Fahrscheinautomaten aus. Beim Beantragen der Ermäßigung konnten an den Automaten allerdings nicht nur die eigenen personenbezogenen Daten angezeigt, sondern auch die Daten von Personen abgerufen werden, die im gleichen Wohnhaus lebten und ebenfalls in der Datenbank erfasst waren. Die spanische Datenschutzbehörde belegte die örtliche Behörde wegen der rechtswidrigen Offenlegung von Daten mit Sanktionen.

Eine zweite Tendenz besteht dagegen in der Ansicht, dass die Vereinfachung von Verwaltungsprozessen zwangsläufig mit einem gewissen Verlust an Kontrolle über die eigenen personenbezogenen Daten der Benutzer einhergeht. Die Anforderungen einer schnelleren elektronischen Verwaltung und die Anforderungen einer „klassischen" Aufklärung der Bürger konnten nicht gleichzeitig erfüllt werden. Drei Länder (Portugal, Deutschland und Italien) sind der Ansicht, dass die Kontrolle der Bürger über ihre Daten nicht unbedingt eine Folge der Entwicklung der elektronischen Verwaltung sei. In diesem Zusammenhang sieht die französische Datenschutzbehörde die Gefahr, dass diese Kontrolle in der Praxis häufig nur suggeriert wird. Die Benutzer könnten zu der irrigen Annahme gelangen, dass sie ihre Daten kontrollieren, während Einzelpersonen tatsächlich durch Gesetze und sonstige Rechtsvorschriften verpflichtet sein könnten, Daten an die Verwaltungen weiterzugeben. In diesem Sinne vertritt auch die portugiesische Datenschutzbehörde die Ansicht, dass selbst wenn die elektronische Verwaltung das Recht der Bürger auf den Zugriff auf ihre jeweils online verfügbaren Daten teilweise unterstützen könnte, die Besucher keine weitere Kontrolle über ihre persönlichen Daten ausüben würden; dies gelte um so mehr, wenn die Zustimmung der Bürger zur Weitergabe ihrer Daten an Dritte innerhalb der Verwaltung als Maßstab genommen werde**.**

EINRICHTUNG VON KONTROLLBEHÖRDEN FÜR DEN DATENSCHUTZ SPEZIELL BEI PROJEKTEN DER ELEKTRONISCHEN VERWALTUNG

Außer von Belgien sowie in gewissem Umfang von Finnland wurde die Einrichtung einer besonderen Datenschutzbehörde für Angelegenheiten der elektronischen Verwaltung von keinem Land auch nur erwähnt. Die bereits bestehenden Datenschutzbehörden scheinen naturgemäß geeignet, Standpunkte zu Projekten der elektronischen Verwaltung vorzutragen, die für den Datenschutz von Bedeutung sind.

Sonstige Behörden können hinzugezogen werden, um Fragen des Datenschutzes im Bereich der elektronischen Verwaltung zu untersuchen. Im Vereinigten Königreich z.B. kann der Ombudsmann der Regierung Beschwerden von Einzelpersonen betreffend Aktivitäten der Verwaltung einschließlich Aktivitäten im Bereich der elektronischen Verwaltung nachgehen. In Finnland überwacht die Regulierungsbehörde für den Bereich Telekommunikation die Einhaltung der maßgeblichen Bestimmungen durch die Zertifizierungs- und Telekommunikationsbehörden im Allgemeinen; für Fragen der elektronischen Erfassung sind Fachbehörden zuständig. Manchmal (z.B. in Dänemark) übernimmt die Datenschutzbehörde auf Antrag der zuständigen öffentlichen Stellen ausdrücklich zusätzliche Kompetenzen in Bezug auf die Genehmigung von Sicherheitslösungen im Bereich der elektronischen Verwaltung. In allen Fällen wird hingegen unter keinen Umständen die Kompetenz zur Überwachung dieser Tätigkeiten in Verbindung mit den Datenschutzbestimmungen zwischen den Datenschutzbehörden und sonstigen Behörden aufgeteilt.

In Belgien wurde die Möglichkeit einer geteilten Zuständigkeit allerdings überprüft. Zurzeit läuft ein Projekt zur Einrichtung eines von der Datenschutzbehörde unabhängigen Prüfungsrates bestehend aus Genehmigungsausschüssen für den Zugang zu nicht öffentlichen Daten, die von der Verwaltung in der Datenbank „*banque carrefour des entreprises*“ gespeichert werden. Zunächst waren diese Genehmigungsausschüsse von der Kommission getrennt. Letztere hat in ihrer Entscheidung betreffend den Aufbau dieser Datenbank gefordert, dass diese Ausschüsse innerhalb der Kommission eingerichtet werden. Insbesondere hat die Kommission betont, dass die Schaffung getrennter Kommissionen die erforderliche Einheitlichkeit des Ansatzes beeinträchtige, die besonders auf institutioneller Ebene die Überwachung des Schutzes der Privatsphäre kennzeichnen sollte. Die belgische Kommission erklärt der Regierung, ihr erscheine wesentlich, dass die Folgen dieser Entscheidung gut überdacht seien, wenn die Regierung beabsichtige, eine Politik der elektronischen Verwaltung mit Anwendungen zu entwickeln, die später in andere Bereiche der Verwaltung übernommen werden können sollen (z.B. der elektronische Ausweis). Angesichts der zu erwartenden Zunahme entsprechender Fragen hält es die Kommission für entscheidend, dass die Fragen, die sich aus der Einrichtung dieser neuen Datenbank hinsichtlich der Grundrechte und -freiheiten der Bürger ergeben, in größtmöglichem Umfang in einer einzigen Einrichtung untersucht werden können. Im derzeitigen Projekt werden diese Ausschüsse ab sofort innerhalb der Kommission angesiedelt. An den Ausschüssen sind jeweils eine bestimmte Anzahl an Mitgliedern der Kommission sowie Vertreter und / oder Experten der betreffenden Sektoren beteiligt.

Geschehen zu Brüssel, am 8. Mai 2003
Für die Arbeitsgruppe
Der Vorsitzende
Stefano RODOTA